

Andrew Chi-Chih Yao

Department of Computer Science, Princeton University, Princeton, New Jersey 08544

Received May 20, 1996

We show that any algebraic computation tree or any fixed-degree algebraic tree for solving the membership question of a compact set  $S \subseteq R^n$  must have height greater than  $\Omega(\log(\beta_i(S))) - cn$  for each  $i$ , where  $\beta_i(S)$  is the  $i$ th Betti number. This generalizes a well-known result by Ben-Or who proved this lower bound for the case  $i = 0$ , and a recent result by Björner and Lovász who proved this lower bound for all  $i$  for linear decision trees. © 1997 Academic Press

## 1. INTRODUCTION

Problems in geometry and combinatorial optimization can often be phrased as *membership* problems for sets  $S \subseteq R^n$ : given an input  $\mathbf{x} = (x_1, x_2, \dots, x_n) \in R^n$ , decide whether  $\mathbf{x} \in S$ . Two standard complexity models for the membership problems are the fixed-degree algebraic tree model and the algebraic computation tree model (see, e.g., [SY82; Be83]).

In both models, an algorithm is a decision tree whose nodes perform certain algebraic tests, and each leaf of the tree contains either a YES or NO answer. In a *degree- $d$  algebraic tree* ( $d \geq 1$ ), each internal node performs a ternary test of the form  $p(\mathbf{x}) : 0$ , where  $p$  is any polynomial with real coefficients and of degree not exceeding  $d$ . In an *algebraic computation tree*, an internal node  $v$  performs either an *arithmetic operation*  $z \leftarrow z' \text{ op } z''$  (where  $\text{op} \in \{+, -, *, /\}$ ) or a ternary *branching test*  $z' : 0$ , where  $z$  is a programming variable created at node  $v$ , and  $z', z''$  are either constants, input variables  $x_i$ , or programming variables already created on the path from the root to  $v$ . An algorithm solves the membership problem for  $S$  if, for every input  $\mathbf{x}$ , the path from the root leads to a leaf with the correct yes–no answer stored at the leaf. We use the term *algebraic decision trees* as an abbreviation for both algebraic computation trees and fixed-degree algebraic trees.

Let  $C_d(S)$  and  $C(S)$  denote the complexities, i.e., the minimum heights of any tree for solving the membership problem for  $S$ , in the degree- $d$  algebraic tree and the

algebraic computation tree models. There is a wealth of literature on the algebraic decision tree complexity for the membership problems (see, e.g., [DL75; SY82; Be83; BLY92; Y92; GKV93] and references therein).

A general approach to derive lower bounds in this area is to establish links between the computational complexity for  $S$  and well-known topological (or geometrical) properties of  $S$ . Dobkin and Lipton [DL75] showed that  $\beta_0(S)$ , the number of path-connected components of  $S$ , is an important topological property from this viewpoint; they proved that  $C_1(S) \geq \Omega(\log \beta_0(S))$ ; i.e., any algebraic tree using linear tests requires at least  $\Omega(\log \beta_0(S))$  tests to solve the membership problem for  $S$ . Steele and Yao [SY82] extended this bound to general fixed-degree algebraic trees, showing  $C_d(S) + n \log C_d(S) \geq \Omega(\log \beta_0(S))$ . Ben-Or [Be83] improved these bounds, showing that both  $C_d(S)$  (for fixed  $d$ ) and  $C(S)$  are at least  $\Omega(\log \beta_0(S))$ . An intriguing question asked in [Be83] was: would the higher Betti numbers  $\beta_i(S)$  ( $i > 0$ ), which describe subtler topological properties of  $S$ , provide lower bounds to  $C_d(S)$  and  $C(S)$ ?

Björner, Lovász, and Yao [BLY92] made a step towards answering this question, showing that  $C_1(S) \geq \Omega(\log |\chi(S)|)$ , where  $\chi(S) = \sum_{i \geq 0} (-1)^i \beta_i(S)$  is a special alternating sum of  $\beta_i(S)$  known as the *Euler characteristic*. They used this bound to show that any linear decision trees must use at least  $\Omega(n \log(n/k))$  tests to solve the “ $k$ -equal problem”—the problem of deciding whether there are  $k$  identical elements out of  $n$  input numbers. This was extended in Yao [Y92] to general algebraic trees, in which it was shown that  $C_d(S), C(S) \geq \Omega(\log |\chi(S)|) - cn$  for all fixed  $d$ .

Recently, Björner and Lovász [BL92] made another step towards linking  $\beta_i$  with computational complexity, showing that for linear decision trees  $\Omega(\log \beta_i(S))$  is a lower bound for all  $i \geq 0$ ; more precisely, they showed  $C_1(S) \geq \log_3(\sum_{i \geq 0} \beta_i(S))$ .

In this paper, we extend [BL92] to general algebraic trees, thus giving a fairly complete answer to the question raised in [Be83] concerning the link between algebraic decision tree complexity and higher Betti numbers. We proved that, for any compact set  $S \subseteq R^n$ ,  $C_d(S), C(S) \geq \Omega(\log(\sum_{i \geq 0} \beta_i(S))) - cn$  (for all fixed  $d$ ). We also apply this

\* This research was supported in part by the National Science Foundation under Grant CCR-9301430.

bound to a class of problems, demonstrating in particular that sometimes tight lower bounds for problems can be obtained in an unexpectedly easy way.

We remark that the algebraic decision tree models discussed here aim at modeling sequential computations. For parallel models using algebraic branching operations, there are also lower bounds involving Betti numbers (see [Y82; MP93; MMP94]).

## 2. AN OVERVIEW OF THE PROOFS

In order to prove the above-mentioned results, we need to formulate them in a more general setting. We will introduce the needed concepts in the Section 3, and state the main theorems in Section 4. The proofs are given in Sections 5–8.

It is possible to explain in a few paragraphs the critical new insights we employ for the proofs. This section is devoted to an exposition of these insights, without getting into technical details. For concreteness, we consider only fixed-degree algebraic trees.

A general methodology for proving lower bounds is to seek a *weight measure*  $\nu$  which associates with each set  $A \subseteq R^n$  a real number  $\nu(A) \geq 0$ . Two desirable properties are:

- (a) the measure is subadditive, i.e.,  $\nu(A \cup B) \leq \nu(A) + \nu(B)$  for disjoint  $A, B$ ; and
- (b) there is an upper bound  $\exp(O(m+n))$  on  $\nu(A)$  if the set  $A$  can be built with  $m$  polynomial inequalities or equalities of degree  $d$  (fixed  $d$ ).

Let  $S \subseteq R^n$  and let  $T$  be a degree- $d$  algebraic tree for the membership question of  $S$ . Let  $V_l \subseteq R^n$  denote the set of inputs reaching a leaf  $l$ . Then by definition  $S$  must be the disjoint union of  $V_l$  over all leaves  $l$  with a “yes” answer. It follows from (a) and (b) that  $\nu(S) \leq (\# \text{ of yes leaves}) \cdot \exp(O(m+n)) \leq 3^m \exp(O(m+n))$ , where  $m$  is the height of  $T$ . This leads to the desired lower bound  $m \geq \Omega(\log(\nu(S))) - cn$ . It works for the case when  $\nu$  is  $\beta_0$ , and when  $\nu$  is the Euler characteristic  $\chi$ .

For Betti numbers  $\beta_i$  with  $i > 0$ , requirement (a) becomes an essential obstacle. Two disjoint sets with small Betti numbers can acquire a substantial jump in Betti numbers when they are unioned together. For example, consider the set  $X$  defined as  $\{(0, y), (1, y), (x, i) \mid 0 \leq y \leq m, i \in \{0, 1, 2, \dots, m\}, 0 < x < 1\}$ , where  $m$  is large. One can write  $X$  as the disjoint union of  $A$  and  $B$ , where  $A = \{(0, y) \mid 0 \leq y \leq m\}$  and  $B = S - A$  (see Fig. 1). It is clear that  $\beta_0(A) = \beta_0(B) = 1$ ,  $\beta_i(A) = \beta_i(B) = 0$  for all  $i > 0$ . However, the Betti numbers of  $X$  are  $\beta_0(X) = 1$ ,  $\beta_1(X) = m$ ,  $\beta_i(X) = 0$  for  $i > 1$ , where the large  $\beta_1$  value comes from the  $m$  independent loops in  $X$ .

To overcome this obstacle, we observe that the  $m$  loops in  $X$  actually have not disappeared without a trace in  $B$ . In

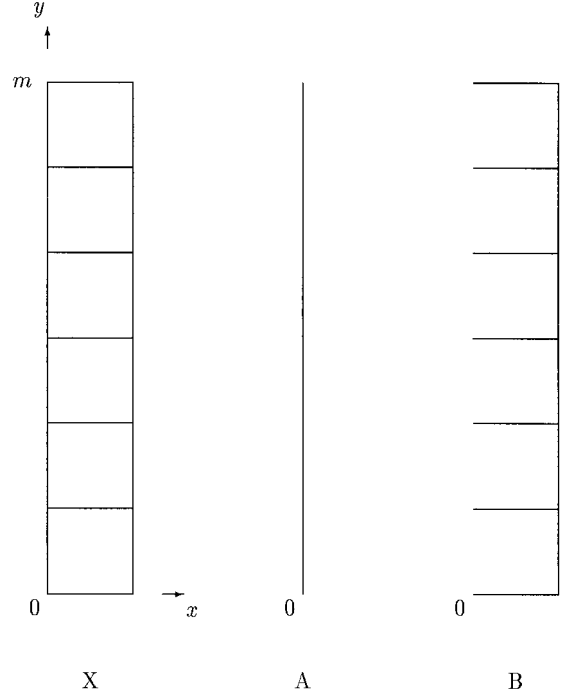


FIG. 1. Betti numbers are not subadditive.

fact, if we take the  $m$  points in the closure of  $B$ , but not in  $B$  itself (i.e.,  $(0, i)$  for  $i \in \{0, 1, 2, \dots, m\}$ ), and glue them together as one point, we get back in  $B$  the  $m$  missing loops. This suggests that we use for  $\nu(S)$ , not  $\beta_i(S)$ , but the *relative Betti numbers*  $\beta_i(\bar{S}, \bar{S} - S)$ , which for our purpose are essentially the Betti numbers of  $\bar{S}$  with all the points in  $\bar{S} - S$  glued into one point. We can show that this  $\nu$  is indeed subadditive for the type of sets we are interested in.

To satisfy requirement (b), we use the standard bounds on the Betti numbers of algebraic sets as in previous investigations. Some additional arguments are needed in the present case, due to the fact that we need to bound, not the Betti numbers, but the relative Betti numbers  $\beta_i(\bar{V}_l, \bar{V}_l - V_l)$ . The sets  $\bar{V}_l, \bar{V}_l - V_l$  do not have a natural simple representation in degree- $d$  polynomial constraints and have to be transformed by topological methods before the standard bounds can be applied.

*Remark 1.* In [BL92]  $\beta_i(Y)$  is used as the measure  $\nu(Y)$  (where  $Y$  are polyhedra). The obstacle mentioned above does not arise because the proof manages to discuss only sets  $Y$  that are open relative to the affine subspaces spanned by  $Y$ . (Thus, for the set  $X$  discussed earlier, the proof would involve  $\beta_i(R^2 - X)$ , instead of  $\beta_i(X)$ .) Their method depends critically on the fact that only linear objects are involved for linear decision trees and seems difficult to generalize to general algebraic decision trees.

### 3. BACKGROUND

An *algebraic set* in  $R^n$  is the set of points  $\mathbf{x} \in R^n$  satisfying a finite set of polynomial equations. The following bound due to Oleinik–Petrovsky–Milnor–Thom is well known.

LEMMA 1 [OP49; Ol52; Mi64; Th65]. *Let  $S = \{\mathbf{x} \mid f_i(\mathbf{x}) = 0, 1 \leq i \leq r\} \subseteq R^n$ . Then all the Betti numbers of  $S$  are finite, and  $\sum_{i \geq 0} \beta_i(S) \leq d(2d-1)^{n-1}$ , where  $d$  is the maximum degree of any  $f_i$ .*

Let  $\hat{R}^n$  be the Euclidean space  $R^n$  compactified by adjoining to it an element  $\omega \notin R^n$  (point at infinity). It is convenient to think of  $\hat{R}^n$  as an  $n$ -dimensional sphere in  $R^{n+1}$ . Using the notation in [Y92], let  $J_{n+1} \subseteq R^{n+1}$  denote the  $n$ -dimensional sphere centered at  $(0, 0, \dots, 0, 2/3)$  with radius  $\frac{1}{3}$ . Let  $\varphi_n: \hat{R}^n \rightarrow R^{n+1}$  be the inverse stereographic map, given by  $\varphi_n(\omega) = (0, 0, \dots, 0, 1)$ , and  $\varphi_n(x_1, x_2, \dots, x_n) = (x_1(1 - y_{n+1}), x_2(1 - y_{n+1}), \dots, x_n(1 - y_{n+1}), y_{n+1})$ , where  $y_{n+1}$  is the unique solution to the system of constraints  $0 < y_{n+1} < 1$  and  $\sum_{1 \leq i \leq n} x_i^2(1 - y_{n+1})^2 + (y_{n+1} - \frac{2}{3})^2 = \frac{1}{9}$ . Then  $\varphi_n$  is a homeomorphism from  $\hat{R}^n$  onto  $J_{n+1}$ . Geometrically, if we identify  $\tilde{\mathbf{x}} = (x_1, x_2, \dots, x_n)$  with the point  $(x_1, x_2, \dots, x_n, 0)$  and draw a line in  $R^{n+1}$  between it and the north pole of  $J_{n+1}$ , then  $\varphi_n(\mathbf{x})$  is the unique point where the line intersects  $J_{n+1}$ .

A set  $S \subseteq \hat{R}^n$  is called *semi-algebraic* if its image  $\varphi_n(S)$  is a semi-algebraic set in  $R^{n+1}$ . Clearly, if  $S$  does not contain  $\omega$ , this usage agrees with the standard meaning of being a semi-algebraic set in  $R^n$ . In this paper, unless otherwise specified, the compactified space is assumed to be the underlying space.

LEMMA 2 (See [Y92]). *If  $S \subseteq \hat{R}^n - \{\omega\}$  is defined by  $r$  degree- $d$  polynomial equalities and  $s$  degree- $d$  polynomial strict inequalities, then  $\varphi_n(S) \subseteq R^{n+1}$  can be described by  $r+1$  degree- $d'$  polynomial equalities and  $s+2$  degree- $d$  polynomial strict inequalities, where  $d' = \max\{d, 2\}$ .*

For any set  $S \subseteq \hat{R}^n$ , let  $\delta S = \bar{S} - S$ , where  $\bar{S}$  is the closure of  $S$  (with respect to the topology of  $\hat{R}^n$ ). Let  $\beta_i(S)$  denote the  $i$ th Betti number of  $S$ , and  $\beta'_i(S)$  denote the rank of the  $i$ th relative homology group  $H_i(\bar{S}, \delta S)$ . Note that  $\beta'_i(S) = \beta_i(S)$  if  $S$  is closed (in the topology of  $\hat{R}^n$ ).

A set in  $\hat{R}^n$  is said to be *semi-closed* if it can be expressed as the difference of two closed sets, or equivalently, as the intersection of an open set and a closed set. Clearly, if  $S$  and  $W$  are semi-closed, then  $S \cap W$  is semi-closed. The next simple fact will be useful.

LEMMA 3. *If  $S$  is a semi-closed set in  $\hat{R}^n$ , then  $\delta S$  is closed.*

*Proof.* Let  $X = A - B$ , where  $A, B$  are closed. Let  $p$  be any point in  $\bar{\delta X}$ . We need to prove  $p \in \delta X$ . Clearly,  $p \in \bar{X}$ , since  $\bar{\delta X} \subseteq \bar{X}$ . Thus, it suffices to prove  $p \notin X$ . Assume that  $p \in X = A - B$ ; we will derive a contradiction. Let  $V$  be an

open neighborhood of  $p$  such that  $V \cap B = \emptyset$ . Let  $p_1, p_2, \dots$ , be a sequence of points in  $\delta X \cap V$  that converges to  $p$ . Then  $p_i \in V \cap \bar{X} \subseteq V \cap \bar{A} = V \cap A$ . Thus,  $p_i \in A - B = X$ , which is a contradiction. ■

### 4. THE RESULTS

Let  $T$  be any algebraic decision tree for solving some membership problem in  $R^n$ . For each leaf  $l$ , let  $V_l \subseteq R^n$  denote the set of input points  $\mathbf{x} \in R^n$  reaching  $l$ . Let  $L_{T, \text{yes}}$  be the set of all YES leaves, and  $L_{T, \text{no}}$  be the set of all NO leaves.

THEOREM 1. *Let  $S \subseteq \hat{R}^n$  be a semi-closed semi-algebraic set not containing  $\omega$ . Any algebraic decision tree  $T$  for solving the membership question of  $S$  must satisfy  $\sum_{l \in L_{T, \text{yes}}} \beta'_i(V_l) \geq \beta'_i(S)$  for all  $i \geq 0$ .*

Remark 2. Any algebraic decision tree for  $S$  can be turned into one for  $R^n - S$ , by exchanging the yes–no answers at the leaves. Thus, Theorem 1 implies that  $\sum_{l \in L_{T, \text{no}}} \beta'_i(V_l) \geq \beta'_i(R^n - S)$  for all  $i \geq 0$ . This proves a version of a conjecture made by Björner and Lovász [BL 92, Conjecture 2.5]. (The original conjecture has  $\beta_i$  instead of  $\beta'_i$ .)

Remark 3. For the case of linear decision trees (i.e.,  $d = 1$ ), each  $V_l$  is a convex polyhedron of certain dimension (call it  $\dim(V_l)$ ). Thus, for  $i \geq 1$ ,  $\beta'_i(V_l) = \delta_{i, \dim(V_l)}$ . It follows that, for  $i \geq 1$ , the number of leaves with  $i$ -dimensional  $V_l$  is greater than or equal to  $\beta'_i(S)$ . (This is similar to the main result proved in [BL92].)

THEOREM 2. *There exist positive constants  $\lambda, \eta, \lambda_d, \eta_d$  such that*

$$C(V_{\mathcal{A}}) \geq \lambda \log_2 \left( \sum_{i \geq 0} \beta'_i(S) \right) - \eta n$$

$$C_d(V_{\mathcal{A}}) \geq \lambda_d \log_2 \left( \sum_{i \geq 0} \beta'_i(S) \right) - \eta_d n,$$

for all  $d \geq 1$ .

Remark 4. If  $S$  is a compact set as a subset of  $R^n$ , then  $\beta'_i(S) = \beta_i(S, \emptyset) = \beta_i(S)$  for all  $i$ . Thus, Theorem 2 implies the result about the membership question for compact sets  $S$  as stated in the abstract.

The next results applies Theorem 2 to yield lower bounds for a class of problems. Let  $\mathcal{A} = \{K_1, K_2, \dots, K_t\}$  be any affine subspace arrangement in  $R^n$ . A subcollection  $\mathcal{F} \subseteq \mathcal{A}$  is called a *free* subset of  $\mathcal{A}$  if  $Y_{\mathcal{F}} \equiv \bigcap_{K \in \mathcal{F}} K$  is nonempty and that (a)  $\text{codim}(Y_{\mathcal{F}}) = \sum_{K \in \mathcal{F}} \text{codim}(K)$ , and (b) for all  $K_j \notin \mathcal{F}$ ,  $Y_{\mathcal{F}} \not\subseteq K_j$ . Let  $N_{\mathcal{A}}$  be the number of free subsets of  $\mathcal{A}$ .

There is a large class of membership problems for which our method gives rise to lower bounds in an appealing

combinatorial form. An *affine subspace arrangement*  $\mathcal{A} = \{K_1, K_2, \dots, K_t\}$  in  $R^n$  is a finite collection of nonempty affine subspaces  $K_i$  of  $R^n$ . We assume that  $K_i \not\subseteq K_j$  for all  $i \neq j$ . Let  $V_{\mathcal{A}} = \bigcup_{1 \leq i \leq t} K_i$ . There is an extensive literature on the topological structures of affine subspace arrangements and their associated  $V_{\mathcal{A}}$  (see Björner [Bj92] for a comprehensive survey). Each affine subspace arrangement  $\mathcal{A}$  gives rise to a natural membership question, that for the set  $V_{\mathcal{A}}$ .

**THEOREM 3.** *Let  $\mathcal{A}$  be any affine subspace arrangement in  $R^n$ . Then*

$$C(V_{\mathcal{A}}) \geq \lambda \log_2 N_{\mathcal{A}} - \eta n$$

$$C_d(V_{\mathcal{A}}) \geq \lambda_d \log_2 N_{\mathcal{A}} - \eta_d n,$$

for all  $d \geq 1$ .

*Remark 5.* As discussed in [BLY92], the “ $k$ -equal problem” can be phrased as the membership question for  $\mathcal{V}_{\mathcal{A}}$ , where  $\mathcal{A} = \{K_{i_1, i_2, \dots, i_k} \mid 1 \leq i_1 < i_2 < \dots < i_k \leq n\}$  is the affine subspace arrangement with  $K_{i_1, i_2, \dots, i_k}$  being the subspace defined by  $x_{i_1} = x_{i_2} = \dots = x_{i_k}$ . It was observed in [BL92] that Betti number bounds lead to somewhat stronger bounds than the Euler characteristic bounds in [BLY92], due to our knowledge about  $\beta_i$  for this  $\mathcal{V}_{\mathcal{A}}$  (see Björner and Welker [BW92]). We now demonstrate that the Betti numbers bounds (in the form of Theorem 3) are also simpler to use in this case. It is easy to see that there are at least

$$\binom{n}{k, k, \dots, k} \Big/ (n/k)! \approx (n/k)^n / (n/k)! \\ \approx (n/k)^{n(1-1/k)}$$

free subsets of  $\mathcal{A}$ . Theorem 3 immediately gives  $\Omega(\log N_{\mathcal{A}}) - cn = \Omega(n \log(n/k)) - cn$  as a lower bound to the complexity of solving the “ $k$ -equal problem.”

*Remark 6.* As another example, consider the following  *$k$ -matching-equal problem*: given an input  $\mathbf{x} = (x_{i,j} \mid 1 \leq i, j \leq n) \in R^{n^2}$ , decide whether there exists a  $k$ -matching  $\{(i_1, j_1), (i_2, j_2), \dots, (i_k, j_k)\}$  such that  $x_{i_1, j_1} = x_{i_2, j_2} = \dots = x_{i_k, j_k}$ . Let  $\mathcal{M}_{k,n}$  denote the natural affine subspace arrangement corresponding to it.

For the case  $k = n$ , it is easy to see that  $N_{\mathcal{M}_{n,n}}$  is at least as large as  $1/n!$  times the number of Latin squares of dimension  $n$ . It is known from Hall [Ha48] (for more information see [BR91]) that the number of such Latin squares is  $\geq n!(n-1)! \dots 2! 1! = e^{\theta(n^2 \log n)}$ . It follows from Theorem 3 and an obvious upper bound using sorting that, in this case, the algebraic decision tree complexity for the  $k$ -matching-equal problem is  $\Theta(n^2 \log n)$ . This can be extended to

prove that the algebraic decision tree complexity for the  $k$ -matching-equal problem is  $\Theta(n^2 \log n)$  for all  $2 \leq k \leq n$ .

## 5. PROOF OF THEOREM 1

We first state a simple fact from algebraic topology (see, e.g., [Ro, Corollary 8.43]).

**LEMMA 4.** *Let  $K \subseteq \hat{R}^n$  be a simplicial complex, and let  $V, W, V \cap W$  be subcomplexes of  $K$ . Then  $\beta_i(W, V \cap W) = \beta_i(V \cup W, V)$  for all  $i \geq 0$ .*

The next lemma gives the crucial subadditive property of Betti numbers needed for the proof of the theorem. Let  $X \subseteq \hat{R}^n$  be a semi-algebraic set not containing  $\omega$  (the point at infinity), and let  $f$  be a polynomial in  $n$  variables. Let  $A$  be the set of points  $\mathbf{x}$  in  $X$  satisfying  $f(\mathbf{x}) \leq 0$ , and  $B = X - A$ .

**LEMMA 5.** *If  $X$  is semi-closed, then  $\beta'_i(X) \leq \beta'_i(A) + \beta'_i(B)$  for all  $i \geq 0$ .*

*Proof.* A basic fact from algebraic topology (see [Ro, Theorem 5.9]) states that, if  $X_1 \supseteq X_2 \supseteq X_3$ , then with the natural interpretation,

$$\dots \rightarrow H_i(X_2, X_3) \rightarrow H_i(X_1, X_3) \rightarrow H_i(X_1, X_2) \rightarrow \dots$$

is part of an exact sequence. This implies

$$\beta_i(X_1, X_3) \leq \beta_i(X_1, X_2) + \beta_i(X_2, X_3).$$

Let  $X_1, X_2, X_3$  be respectively the sets  $\bar{X}, \bar{A} \cup \delta X$ , and  $\delta X$ . We obtain

$$\beta_i(\bar{X}, \delta X) \leq \beta_i(\bar{X}, \bar{A} \cup \delta X) + \beta_i(\bar{A} \cup \delta X, \delta X). \quad (1)$$

We claim that

$$\beta_i(\bar{X}, \bar{A} \cup \delta X) = \beta_i(\bar{B}, \delta B), \quad (2)$$

$$\beta_i(\bar{A} \cup \delta X, \delta X) = \beta_i(\bar{A}, \delta A). \quad (3)$$

To prove (3), let  $W = \bar{A}$ ,  $V = \delta X$ . (Note that  $\delta X$  is a closed set by Lemma 3.) Then  $V \cap W = \bar{A} \cap (\bar{X} - X) = \bar{A} \cap (\bar{A} - X) = \bar{A} - X = \bar{A} - A = \delta A$ . Since  $V, W, V \cap W$  are all semi-algebraic sets in  $\hat{R}^n$  (regarded as the sphere  $S^n \subseteq R^{n+1}$ ), one can find a simultaneous simplicial triangulation for  $V, W, V \cap W, V \cup W$  (see, e.g., [Hi75]). As these sets are closed, they are simplicial subcomplexes of the simplicial complex  $K = V \cup W$ . Using Lemma 4, we obtain immediately (3). Eq. (2) can be similarly proved.

It follows from (1)–(3) that  $\beta_i(\bar{X}, \delta X) \leq \beta_i(\bar{A}, \delta A) + \beta_i(\bar{B}, \delta B)$ . ■

We now prove Theorem 1. For each node  $v \in T$ , let  $L_v$  be the set of leaves  $l \in L_{T, \text{yes}}$  that are descendants of  $v$ . Let  $S_v = \bigcup_{l \in L_v} V_l$ . Note that  $S_v$  is semi-closed, since it can be

written in the form  $S \cap F \cap G$ , where  $F, G \subseteq \hat{R}^n - \{\omega\}$  are semi-closed;  $F$  is defined by a finite set of polynomial equations and  $G$  by a finite set of polynomial (strict) inequalities.

We claim that, for each  $v$ ,  $\sum_{l \in L_v} \beta'_i(V_l) \geq \beta'_i(S_v)$ . Note that  $v = \text{root}$  gives the theorem. We prove the claim by induction on the size  $|L_v|$ . The claim is obviously true for  $|L_v| = 0$ . If  $|L_v| = 1$ , let  $l$  be the unique leaf contained in  $L_v$ ; clearly,  $V_l = S_v$  and the claim is true. Let  $|L_v| > 1$ . Denote by  $v_1, v_2, v_3$  the children of  $v$  corresponding to the branches  $f(\mathbf{x}) < 0, f(\mathbf{x}) = 0$ , and  $f(\mathbf{x}) > 0$ . (For fixed-degree algebraic trees,  $f$  is the polynomial test function associated with  $v$ ; for algebraic computation trees,  $f = pq$ , where  $p/q$  is the rational function corresponding to the value acquired by the program variable  $z_v$  at  $v$ .) By the induction hypothesis,  $\sum_{l \in L_{v_j}} \beta'_i(V_l) \geq \beta'_i(S_{v_j})$  for  $1 \leq j \leq 3$ . To complete the inductive step, it suffices to prove that

$$\sum_{1 \leq j \leq 3} \beta'_i(S_{v_j}) \geq \beta'_i(S_v). \quad (4)$$

By definition,  $S_{v_1} = S_v \cap \{\mathbf{x} \mid f(\mathbf{x}) < 0\}$ ,  $S_{v_2} = S_v \cap \{\mathbf{x} \mid f(\mathbf{x}) = 0\}$ , and  $S_{v_3} = S_v \cap \{\mathbf{x} \mid f(\mathbf{x}) > 0\}$ . Apply Lemma 5 with  $A = S_{v_1} \cup S_{v_2}$  and  $B = S_{v_3}$ , we have

$$\beta'_i(S_v) \leq \beta'_i(S_{v_1} \cup S_{v_2}) + \beta'_i(S_{v_3}).$$

Similarly, we can obtain

$$\beta'_i(S_{v_1} \cup S_{v_2}) \leq \beta'_i(S_{v_1}) + \beta'_i(S_{v_2}).$$

The above two inequalities imply (4) immediately. This completes the inductive step, and the proof of Theorem 1.  $\blacksquare$

## 6. TWO LEMMAS

We derive in this section two preliminary lemmas needed for proving Theorem 2. Let  $r, s \geq 0$  be integers, and let  $f_i(\mathbf{x}), g_j(\mathbf{x})$  be any degree- $d$  polynomials in  $n$  variables, for  $1 \leq i \leq r, 1 \leq j \leq s$ . We prove upper bounds on the Betti numbers of semi-algebraic sets defined by constraints involving  $f_i, g_j$ .

**LEMMA 6.** *Let  $W = \{\mathbf{x} \mid f_i(\mathbf{x}) = 0, g_j(\mathbf{x}) \leq 0, 1 \leq i \leq r, 1 \leq j \leq s\} \subseteq \hat{R}^n - \{\omega\}$ . If  $W$  is bounded as a subset of  $R^n$ , then  $\sum_{i \geq 0} \beta_i(W) \leq d(2d-1)^{n+s-1}$ .*

*Proof.* One first uses topological arguments to relate the Betti numbers of  $W$  to some related algebraic sets, and then applies the standard upper bound (Lemma 1 in Section 3) on the Betti numbers of algebraic sets. We give the details below.

Let  $V \subseteq R^{n+s}$  be the set of all  $(\mathbf{x}, \mathbf{z}) = (x_1, \dots, x_n, z_1, \dots, z_s)$  satisfying  $f_i(\mathbf{x}) = 0, g_j(\mathbf{x}) + z_j^2 = 0$  for  $1 \leq i \leq r, 1 \leq j \leq s$ . Let

$V' = V \cap \{(\mathbf{x}, \mathbf{z}) \mid z_j \geq 0, 1 \leq j \leq s\}$ . Note that  $V, V'$  are bounded as subsets of  $R^{n+s}$ , since  $W$  is bounded in  $R^n$  by assumption.

Clearly, the mapping  $\mathbf{x} \rightarrow (\mathbf{x}, \mathbf{z})$  with  $z_j = \sqrt{-g_j(\mathbf{x})}$  is a homeomorphism from  $W$  to  $V'$ . This implies that for all  $i \geq 0$ ,

$$\beta_i(W) = \beta_i(V'). \quad (5)$$

Note also that we have by Lemma 1 that

$$\sum_{i \geq 0} \beta_i(V) \leq d(2d-1)^{n+s-1}. \quad (6)$$

We will now prove

$$\sum_{i \geq 0} \beta_i(V') \leq \sum_{i \geq 0} \beta_i(V). \quad (7)$$

Clearly, Lemma 6 follows from (5)–(7). Let  $\psi': V' \rightarrow V$  be the inclusion map, and  $\psi: V \rightarrow V'$  be the map  $\psi(x_1, \dots, x_n, z_1, \dots, z_s) = (x_1, \dots, x_n, |z_1|, \dots, |z_s|)$ . Then the induced homomorphisms  $\psi'_*: H_*(V') \rightarrow H_*(V)$ ,  $\psi_*: H_*(V) \rightarrow H_*(V')$  have as its composition  $\psi_* \circ \psi'_*$  the identity map from  $H_*(V')$  onto itself. This implies

$$\text{rank}(H_*(V)) \geq \text{rank}(\psi'_*(H_*(V'))) = \text{rank}(H_*(V')),$$

and, hence, (7).  $\blacksquare$

**LEMMA 7.** *Let  $A = \{\mathbf{x} \mid f_i(\mathbf{x}) = 0, g_j(\mathbf{x}) < 0, 1 \leq i \leq r, 1 \leq j \leq s\} \subseteq \hat{R}^n - \{\omega\}$ . Then  $\sum_{i \geq 0} \beta'_i(A) \leq (2d'+1)^{n+2s+5}$ , where  $d' = \max\{d, 2\}$ .*

*Proof.* We assume that  $A$  is a bounded set when considered as a subset of  $R^n$  and prove the following stronger statement:

$$\sum_{i \geq 0} \beta'_i(A) \leq (2d+1)^{n+2s}.$$

If  $A$  is unbounded as a subset of  $R^n$ , we can apply the above bound to its inverse stereographic image  $\varphi_n(A) \subseteq R^{n+1}$ . By Lemma 2, this amounts to replacing  $n$  by  $n+1$ ,  $d$  by  $d'$ ,  $r$  by  $r+1$ , and  $s$  by  $s+2$ , resulting in the bound stated in Lemma 7.

We first give an overview of the proof. By definition,  $\beta'_i(A) = \beta_i(\bar{A}, \delta A)$ . From basic algebraic topology, one can conclude that  $\beta'_i(A) \leq \beta_i(\bar{A}) + \beta_{i-1}(\delta A)$ . Although  $\bar{A}, \delta A$  are semi-algebraic sets, the known upper bounds on the Betti numbers of semi-algebraic sets (such as Lemma 6) cannot be applied directly, since  $\bar{A}, \delta A$  do not have a natural simple representation in terms of the polynomials  $f_i, g_j$ . To overcome this problem, we construct two sets  $A', D$  with simple representations using  $f_i, g_j$  (see below)

and such that  $\beta_i(\bar{A}, \delta A) = \beta_i(A', D)$ . Lemma 6 can then be applied to  $A'$  and  $D$ .

To carry out the above plan, let  $A' \subseteq \hat{R}^n - \{\omega\}$  be the set of all  $\mathbf{x}$  such that  $f_i(\mathbf{x}) = 0$ ,  $g_j(\mathbf{x}) \leq 0$  for all  $1 \leq i \leq r$ ,  $1 \leq j \leq s$ . Let  $D = A' \cap \{\mathbf{x} \mid \prod_{1 \leq j \leq s} g_j(\mathbf{x}) = 0\}$ . Note that  $A', D$  are bounded as sets in  $R^n$ , since  $A$  is bounded as a set in  $R^n$ ;  $A', D$  are also closed (in  $R^n$  as well as in  $\hat{R}^n$ ).

CLAIM.  $\beta_i(\bar{A}, \delta A) = \beta_i(A', D)$ .

To prove the claim, let  $V = D$ ,  $W = \bar{A}$ . It is straightforward to verify that  $V \cap W = \delta A$  and  $V \cup W = A'$ . Now, observe that  $V, W, V \cap W$  are compact semi-algebraic sets in  $R^n$ , and thus can be simultaneously triangulated as simplicial complexes (see [Hi75]). The claim then follows from Lemma 4. ■

It follows from the claim that

$$\beta'_i(A) = \beta_i(A', D). \quad (8)$$

Now, there is an exact sequence

$$\cdots \rightarrow H_i(D) \rightarrow H_i(A') \rightarrow H_i(A', D) \rightarrow H_{i-1}(D) \rightarrow \cdots$$

by basic homology theory (e.g., [Ro88, Theorem 5.8]). Thus, with  $\beta_{-1}(D)$  understood to be 0, we have for all  $i \geq 0$ ,

$$\beta_i(A', D) \leq \beta_i(A') + \beta_{i-1}(D). \quad (9)$$

By Lemma 6,

$$\sum_{i \geq 0} \beta_i(A') \leq d(2d-1)^{n+s-1}. \quad (10)$$

A similar bound on  $\beta_{i-1}(D)$  does not immediately follow from Lemma 6, since one of the defining constraints  $\prod_{1 \leq j \leq s} g_j(\mathbf{x}) = 0$  is of degree  $sd$ . To obtain a good bound, consider the set  $D_1 \subseteq \hat{R}^{n+s} - \{\omega\}$ , defined as the set of all  $(x_1, \dots, x_n, z_1, \dots, z_s)$  satisfying  $f_i(\mathbf{x}) = 0$ ,  $g_j(\mathbf{x}) \leq 0$ ,  $1 \leq i \leq r$ ,  $1 \leq j \leq s$ , and  $z_1 = g_1(\mathbf{x})$ ,  $z_2 = g_2(\mathbf{x})z_1, \dots, z_s = g_s(\mathbf{x})z_{s-1}$ ,  $z_s = 0$ . It is easy to see that  $D_1$  is homeomorphic to  $D$ . Now, one can apply Lemma 6 to  $D_1$  which leads to

$$\begin{aligned} \sum_{i \geq 0} \beta_i(D) &= \sum_{i \geq 0} \beta_i(D_1) \\ &\leq (d+1)(2d+1)^{n+2s-1}. \end{aligned} \quad (11)$$

It follows from (8)–(11) that  $\sum_{i \geq 0} \beta'_i(A) \leq (2d+1)^{n+2s}$ . ■

## 7. PROOF OF THEOREM 2

Without loss of generality, we can assume that  $S \neq \emptyset$ ,  $R^n$ . Let  $d \geq 1$ , and  $T$  be any degree- $d$  algebraic tree for solving

the membership question for  $S$ . Let  $m$  be the height of  $T$ . Clearly,  $m \geq 1$  as  $S \neq \emptyset$ ,  $R^n$ . For each leaf  $l \in L_{T, \text{yes}}$ ,  $V_l$  is the set of all  $\mathbf{x}$  satisfying  $m$  (or fewer) constraints  $f_i(\mathbf{x}) = 0$ ,  $g_j(\mathbf{x}) < 0$ , where  $f_i, g_j$  are the degree- $d$  polynomials employed as tests at nodes along the path from the root to  $l$ . By Lemma 7, we have

$$\sum_{i \geq 0} \beta'_i(V_l) \leq (2d' + 1)^{n+2m+5},$$

where  $d' = \max\{d, 2\}$ . Theorem 1 then implies  $\sum_{i \geq 0} \beta'_i(S) \leq \sum_{l \in L_{T, \text{yes}}} \sum_{i \geq 0} \beta'_i(V_l) \leq |L_{T, \text{yes}}| \cdot (2d' + 1)^{n+2m+5} \leq 3^m \cdot (2d' + 1)^{n+2m+5}$ . Thus,  $m$ , the height of  $T$ , is at least as large as  $\lambda_d \log(\sum_{i \geq 0} \beta'_i(S)) - \eta_d n$  for some positive constants  $\lambda_d, \eta_d$ . This proves Theorem 2 for the case of fixed-degree algebraic trees.

We now turn to the case of algebraic computation trees. The proof follows the same outline, but additional arguments are needed to handle the program variables created at arithmetic nodes.

As discussed in Lubiw [Lu90], one can eliminate all the division arithmetic operations in any algebraic computation tree with at most a constant factor increase in the height of the tree. Essentially, each program variable  $z$  can be simulated by a pair of program variables  $(p, q)$  such that  $z = p/q$  and that only additions, subtractions, and multiplications are used for assignment instructions. From now on, we assume that division operations are not used.

Let  $T$  be any algebraic computation tree which solves the membership problem for  $S$ . Let  $m$  denote the height of  $T$ . We will show

$$m \geq \lambda \log_2 \left( \sum_{i \geq 0} \beta'_i(S) \right) - \eta n \quad (12)$$

for some positive constants  $\lambda, \eta$ .

For each  $l \in L_{T, \text{yes}}$ , let  $V_l$  be the set of all inputs  $\mathbf{x} \in \hat{R}^n - \{\omega\}$  reaching  $l$ . As mentioned in [Be],  $V_l$  are semi-algebraic sets. In fact, one can transform  $T$  into a (possibly) high-degree algebraic tree, by eliminating all arithmetic nodes and replacing the instruction  $z_v : 0$  at each branching node  $v$  with a suitable polynomial test  $p_v(\mathbf{x}) : 0$ , while keeping the original leaves  $l$  with the same  $V_l$ . Thus, by Theorem 1, we have

$$\beta'_i(S) \leq \sum_{l \in L_{T, \text{yes}}} \beta'_i(V_l) \quad (13)$$

for all  $i \geq 0$ .

Let  $l \in L_{T, \text{yes}}$ . We will prove that

$$\sum_{i \geq 0} \beta'_i(V_l) \leq 5^{n+2m+10}. \quad (14)$$

As in the case of fixed-degree trees, (12) follows from (13) and (14) by a standard argument.

Let  $v_1 = \text{root}$ ,  $v_2, \dots, v_{t+1} = l$  be the sequence of nodes along the path  $\xi$  from the root to  $l$ . Clearly,  $t \leq m$ . Let  $\{v_i \mid i \in I\}$ , be the set of arithmetic nodes along  $\xi$ , and let  $I' = \{1, 2, \dots, t\} - I$ . Let  $z_i$ ,  $i \in I$ , be the programming variables created at nodes  $v_i$ .

We agree that, for  $j \in \{1, \dots, n\}$ , the symbol  $z_{-j}$  stands for  $x_j$ ; also, for  $j \in \{n+1, \dots, n'\}$  for some  $n'$ , each  $z_{-j}$  stands for some constant used in the computation tree. With this understanding, each arithmetic node  $v_i$  performs an assignment of the form  $z_i \leftarrow z_j \circ z_k$ , where  $\circ \in \{+, -, *\}$  and  $j, k \in \{-n', -n'+1, \dots, i-1\} - \{0\} - I'$ ; each branching node  $v_i$  performs  $z_j : 0$  for some  $j \in \{-n, -n+1, \dots, i-1\} - \{0\} - I'$ .

Note that  $V_I$  may not be bounded sets in  $R^n$ ; the program variables  $z_i$  take on values that are polynomials in the input variables  $x_1, \dots, x_n$  and may become unbounded in this case. We want to represent  $V_I$  (in fact,  $\varphi_n(V_I)$ ) in the coordinates  $\mathbf{y} = (y_1, y_2, \dots, y_{n+1})$  as a bounded set in  $R^{n+1}$ , and also to replace program variables  $z_i$  by a pair of program variables  $(u_i, w_i)$  whose values are bounded.

We first make a simple observation, which follows from the facts that  $x_j = y_j/(1 - y_{n+1})$  and that  $z_i$  are assigned values which are polynomials in the  $x$ 's. Let us make this explicit. Define  $e_{-i} = 1$ ,  $a_{-i}(\mathbf{y}) = y_i$  for  $1 \leq i \leq n$ , and  $e_{-j} = 0$ ,  $a_{-j}(\mathbf{y}) \equiv z_{-j}$  for  $n < j \leq n'$ . For  $i \in I$  with  $z_i \leftarrow z_j \circ z_k$  being the assignment, we define  $a_i, e_i$  inductively as below. If  $\circ = *$ , then  $e_i = e_j + e_k$  and  $a_i(\mathbf{y}) = a_j(\mathbf{y}) a_k(\mathbf{y})$ . If  $\circ \in \{+, -\}$ , let  $e_i = \max\{e_j, e_k\}$ ;  $a_i(\mathbf{y}) = a_j(\mathbf{y}) \circ ((1 - y_{n+1})^{e_j - e_k} a_k(\mathbf{y}))$  if  $e_j \geq e_k$ , and  $a_i(\mathbf{y}) = ((1 - y_{n+1})^{e_k - e_j} a_j(\mathbf{y})) \circ a_k(\mathbf{y})$  if  $e_j < e_k$ . It is easy to see that one has

*Fact 1.* For each  $i \in I$ , the value assigned to  $z_i$  is equal to  $a_i(\mathbf{y})(1 - y_{n+1})^{-e_i}$ .

For each  $j \in I'$ , let  $z_{\mu(j)} \text{ rel}_j 0$  be the branching label going out to the next node  $v_{j+1}$ . Fact 1 implies

*Fact 2.*  $\varphi_n(V_I)$  is exactly the set of all  $\mathbf{y} \in R^{n+1}$  that satisfy the constraints  $\sum_{1 \leq i \leq n} y_i^2 + (y_{n+1} - 2/3)^2 - 1/9 = 0$ ,  $1 - y_{n+1} > 0$ ,  $y_{n+1} > 0$ , and  $a_{\mu(j)}(\mathbf{y}) \text{ rel}_j 0$  for all  $j \in I'$ .

We now relate  $\varphi_n(V_I)$  to some algebraic set whose Betti numbers can be estimated from Lemma 7. We associate with each  $v_i$ ,  $1 \leq i \leq t$ , one or more polynomial constraints in variables  $y_1, y_2, \dots, y_{n+1}, u_i, w_i$ ,  $i \in I$ . The idea is to separate out the singular part of  $z_i$ , by having  $w_i$  and  $u_i$  taking on the values  $(1 - y_{n+1})^{e_i}$  and  $a_i(\mathbf{y})$ , respectively.

To simplify notations, for each  $1 \leq i \leq n$ , the symbol  $u_{-i}$  stands for  $y_i$ ,  $w_{-i}$  stands for  $1 - y_{n+1}$ . For  $n+1 \leq i \leq n'$ , let  $u_{-i}$  stands for  $z_{-i}$  (which is a constant), and  $w_{-i}$  stands for the constant 1.

*Case A.*  $i \in I'$ . We associate with  $v_i$  the inequality  $f_i(\mathbf{y}, \mathbf{u}, \mathbf{w}) \text{ rel}_i 0$ , where  $f_i$  is the linear polynomial  $u_{\mu(j)}$ .

*Case B.*  $i \in I$  and the assignment is  $z_i \leftarrow z_j * z_k$ . We associate with  $v_i$  two polynomial constraints  $g_i(\mathbf{x}, \mathbf{u}, \mathbf{w}) = 0$  and  $h_i(\mathbf{x}, \mathbf{u}, \mathbf{w}) = 0$ , where  $g_i$  is  $u_i - u_j u_k$  and  $h_i$  is  $w_i - w_j w_k$ .

*Case C.*  $i \in I$  and the assignment is  $z_i \leftarrow z_j \circ z_k$ , where  $\circ \in \{+, -\}$ . We associate with  $v_i$  two polynomial constraints  $g_i(\mathbf{x}, \mathbf{u}, \mathbf{w}) = 0$  and  $h_i(\mathbf{x}, \mathbf{u}, \mathbf{w}) = 0$ . There are two subcases: (a) if  $e_j \geq e_k$ , then  $g_i$  is  $w_k u_i - (w_k u_j \circ w_j u_k)$  and  $h_i$  is  $w_i - w_j$ ; and (b) if  $e_j < e_k$ , then  $g_i$  is  $w_j u_i - (w_k u_j \circ w_j u_k)$  and  $h_i$  is  $w_i - w_k$ .

Furthermore, let  $f_0$  be the polynomial  $\sum_{1 \leq i \leq n} y_i^2 + (y_{n+1} - 2/3)^2 - 1/9$ ,  $g_0$  be the polynomial  $1 - y_{n+1}$ , and  $h_0$  be the polynomial  $y_{n+1}$ .

Note that  $f_i, g_i, h_i$  all have degree at most 2.

Let  $M \subseteq R^{n+2|I|+1}$  be the set of all  $(\mathbf{y}, \mathbf{u}, \mathbf{w})$  satisfying  $f_0(\mathbf{y}, \mathbf{u}, \mathbf{w}) = 0$ ,  $g_0(\mathbf{y}, \mathbf{u}, \mathbf{w}) > 0$ ,  $h_0(\mathbf{y}, \mathbf{u}, \mathbf{w}) > 0$ ,  $f_i(\mathbf{y}, \mathbf{u}, \mathbf{w}) \text{ rel}_i 0$ ,  $g_j(\mathbf{y}, \mathbf{u}, \mathbf{w}) = 0$ ,  $h_j(\mathbf{y}, \mathbf{u}, \mathbf{w}) = 0$  for  $i \in I'$ ,  $j \in I$ . Our next goal is to prove

$$M = \{(\mathbf{y}, a_i(\mathbf{y})(i \in I), (1 - y_{n+1})^{e_i}(i \in I)) \mid \mathbf{y} \in \varphi_n(V_I)\}. \quad (15)$$

We sketch the proof of (15). First one can prove by straightforward induction that, for each  $\mathbf{y} \in R^{n+1}$ , any point  $(\mathbf{y}, \mathbf{u}, \mathbf{w}) \in M$  must satisfy  $u_i = a_i(\mathbf{y})$ ,  $w_i = (1 - y_{n+1})^{e_i}$  for all  $i \in I$ . This shows that  $M$  is equal to the set of all  $(\mathbf{y}, a_i(\mathbf{y})(i \in I), (1 - y_{n+1})^{e_i}(i \in I))$  such that  $f_0(\mathbf{y}, \mathbf{u}, \mathbf{w}) = 0$ ,  $g_0(\mathbf{y}, \mathbf{u}, \mathbf{w}) > 0$ ,  $h_0(\mathbf{y}, \mathbf{u}, \mathbf{w}) > 0$ ,  $f_i(\mathbf{y}, \mathbf{u}, \mathbf{w}) \text{ rel}_i 0$ ,  $g_j(\mathbf{y}, \mathbf{u}, \mathbf{w}) = 0$ ,  $h_j(\mathbf{y}, \mathbf{u}, \mathbf{w}) = 0$  for  $i \in I'$ ,  $j \in I$  when we set  $u_i = a_i(\mathbf{y})$  and  $w_i = (1 - y_{n+1})^{e_i}$ . A comparison with Fact 2 leads to (15).

Note that  $\varphi_n(V_I)$  and  $M$  are bounded as sets in  $R^{n+1}$  and  $R^{n+2|I|+1}$ . The mapping  $\mathbf{y} \rightarrow (\mathbf{y}, a_i(\mathbf{y})(i \in I), (1 - y_{n+1})^{e_i}(i \in I))$  is thus a homeomorphism from  $\varphi_n(V_I)$  onto  $M$ . Furthermore, this maps the subset  $\delta\varphi_n(V_I)$  onto  $\delta M$ . Thus,  $H_*(\varphi_n(V_I), \delta\varphi_n(V_I))$  is isomorphic to  $H_*(M, \delta M)$ . This proves

$$\beta'_i(V_I) = \beta'_i(\varphi_n(V_I)) = \beta'_i(M).$$

But  $M \subseteq R^{n+2|I|+1}$  is defined by degree-2 polynomial equalities and no more than  $|I'| + 2$  strict inequalities. By Lemma 7,  $\sum_{i \geq 0} \beta'_i(M) \leq (2 \cdot 2 + 1)^{n+2|I|+1+2(|I'|+2)+5} \leq 5^{n+2m+10}$ . This proves (14) and completes the proof of Theorem 2.

## 8. PROOF OF THEOREM 3

Some background results are needed. Let  $B_m$  denote the poset formed by all subsets of  $\{1, 2, \dots, m\}$ , ordered by reverse inclusion ( $x \leq y$  if and only if  $x \supseteq y$ ). This poset has a maximum element  $\hat{1} = \emptyset$  and a minimum element  $\hat{0} = \{1, 2, \dots, m\}$ . It is well known that  $\mu_{B_m}(\hat{0}, \hat{1}) = (-1)^m$  (see [St86, Example 3.8.3]).

We also need some results from the theory of subspace arrangements. Let  $\mathcal{L}_{\mathcal{A}}$  be the poset formed by the collection

of all nonempty intersections  $K_{i_1} \cap K_{i_2} \cap \cdots \cap K_{i_p}$ ,  $i_1 < i_2 < \cdots < i_p$ , ordered by reverse inclusion.  $\mathcal{L}_{\mathcal{A}}$  is called the *intersection semilattice*, and it contains a minimum element  $\hat{0} = R^n$ . Let  $\mu_{\mathcal{L}_{\mathcal{A}}}(x, y)$  be the Möbius function defined on  $\mathcal{L}_{\mathcal{A}}$ . The topological structure of  $V_{\mathcal{A}}$  is closely related to the algebraic properties of  $\mathcal{L}_{\mathcal{A}}$  (see, e.g., [Bj92]). For our purpose, the following result is sufficient (essentially due to Goresky and MacPherson [GM88] and given in the present form in Björner and Lovász [BL92]).

*Fact 3.*  $\sum_{i \geq 0} \tilde{\beta}_i(\bar{V}_{\mathcal{A}}) \geq \sum_{\hat{0} < x \in \mathcal{L}_{\mathcal{A}}} |\mu_{\mathcal{L}_{\mathcal{A}}}(\hat{0}, x)|$ , where  $\tilde{\beta}_i$  stands for the  $i$ th *reduced* Betti number.

We can now prove Theorem 3. Observe that, for all  $i \geq 0$ ,  $\beta_i(S, x_0) = \tilde{\beta}_i(S)$  for any set  $S \subseteq \hat{R}^n$  and point  $x_0 \in S$  (see, e.g., [Ro, Theorem 5.17]). It follows that  $\beta'_i(V_{\mathcal{A}}) = \beta_i(\bar{V}_{\mathcal{A}}, \omega) = \tilde{\beta}_i(\bar{V}_{\mathcal{A}})$  for all  $i \geq 0$ . By Fact 3, this means

$$\sum_{i \geq 0} \beta'_i(V_{\mathcal{A}}) \geq \sum_{\hat{0} < x \in \mathcal{L}_{\mathcal{A}}} |\mu_{\mathcal{L}_{\mathcal{A}}}(\hat{0}, x)|. \quad (16)$$

The plan is to show that there are  $N_{\mathcal{A}}$  elements  $x$  with nonvanishing  $\mu_{\mathcal{L}_{\mathcal{A}}}(\hat{0}, x)$ . For each free subset  $\mathcal{F}$  of  $\mathcal{A}$ , let  $x_{\mathcal{F}} \in \mathcal{L}_{\mathcal{A}}$  denote the element  $\bigcap_{K \in \mathcal{F}} K$ . It is easy to verify that the induced poset  $P$  between  $\hat{0}$  and  $x_{\mathcal{F}}$  (inclusive) is isomorphic to the poset  $B_{|\mathcal{F}|}$ . As  $\mathcal{F}$  is free, clearly the value of the Möbius function  $\mu_{\mathcal{L}_{\mathcal{A}}}(\hat{0}, x)$  for any  $x \in P$  is the same as  $\mu_P(\hat{0}, x)$ . Thus,  $\mu_{\mathcal{L}_{\mathcal{A}}}(\hat{0}, x) = \mu_{B_{|\mathcal{F}|}}(\hat{0}, \hat{1}) = (-1)^{|\mathcal{F}|}$ . It follows from (16) that  $\sum_{i \geq 0} \beta'_i(V_{\mathcal{A}}) \geq N_{\mathcal{A}}$ . Theorem 3 now follows from Theorem 2.

## ACKNOWLEDGMENTS

The author thanks Anders Björner and Laci Lovász for communicating to him their results [BL92], which motivated the present work; he also thanks Laci for helpful discussions about Theorem 1. The author thanks Noga Alon and Igor Rivin for useful information on Latin squares.

## REFERENCES

- [Be83] M. Ben-Or, Lower bounds for algebraic computation trees, in “Proceedings, 15th Annual ACM Symposium on Theory of Computing, May 1983,” pp. 80–86.
- [Bj92] A. Björner, Subspace arrangements, in “Proceedings, 1st European Congress of Mathematics, Paris, 1992” (A. Joseph *et al.*, Eds.), Progress in Mathematics, Vol. 119, pp. 321–370, Birkhäuser, Boston, 1994.
- [BL92] A. Björner and L. Lovász, Linear decision trees, subspace arrangements and Möbius functions, *J. Math. Soc.* **7** (1994), 677–706.
- [BLY92] A. Björner, L. Lovász, and A. Yao, Linear decision trees: Volume estimates and topological bounds, in “Proceedings, 24th Annual ACM Symposium on Theory of Computing, May 1992,” pp. 170–177.
- [BW92] A. Björner and V. Welker, The homology of “ $k$ -equal” manifolds and related partition lattices, *Adv. in Math.* **110** (1995), 277–313.
- [BR91] R. Brualdi and H. Ryser, “Computational Matrix Theory,” Cambridge Univ. Press, Cambridge, 1991.
- [DL75] D. Dobkin and R. J. Lipton, On the complexity of computations under varying sets of primitives, in “Automata Theory and Formal Languages” (H. Bradhage, Ed.), Lecture Notes in Computer Science, Vol. 33, pp. 110–117, Springer-Verlag, New York/Berlin, 1975.
- [GM88] M. Goresky and R. MacPherson, “Stratified Morse Theory,” Springer-Verlag, New York, 1988.
- [GKV93] D. Grigoriev, M. Karpinski, and N. Vorobjov, Complexity lower bounds on testing membership to a polyhedron by algebraic decision trees, in “Proceedings of 26th Annual ACM Symposium on Theory of Computing, May 1994.”
- [Ha48] M. Hall, Jr., Distinct representatives of subsets, *Bull. Amer. Math. Soc.* **54** (1948), 958–961.
- [Hi75] H. Hironaka, Triangulation of algebraic sets, in “Proceedings, Symposia in Pure Mathematics,” Vol. 29, pp. 165–185, American Mathematical Society, 1975.
- [Lu90] A. Lubiw, A RAM lower bound for the integer distinctness problem, preprint, 1990.
- [Mi64] J. Milnor, On the Betti numbers of real varieties, *Proc. Amer. Math. Soc.* **15** (1964), 275–280.
- [MP93] J. L. Montaña and L. M. Pardo, Lower bounds for arithmetic networks, *Appl. Algebra Engi. Commun. Comput.* **4** (1993), 1–24.
- [MMP94] J. L. Montaña, J. E. Morais, and L. M. Pardo, Lower bounds for arithmetic networks II: Sum of betti numbers, *Appl. Algebra Engi. Commun. Comput.*, to appear (preprint 1994).
- [Ol51] O. A. Oleinik, Estimates of the Betti numbers of real algebraic hypersurfaces, *Mat. Sb. (N.S.)* **28** (1951), 635–640. [in Russian]
- [OP49] O. A. Oleinik and I. B. Petrovsky, On the topology of real algebraic surfaces, *Izv. Akad. Nauk SSSR* **13** (1949), 389–402 [in Russian]; *Transl. Amer. Math. Soc. (1)* **7** (1962), 399–417.
- [Ro88] J. Rotman, “An Introduction to Algebraic Topology,” Springer-Verlag, New York, 1988.
- [St86] R. P. Stanley, “Enumerative Combinatorics,” Vol. 1, Springer-Verlag, New York, 1988.
- [SY82] M. Steele and A. Yao, Lower bounds for algebraic decision trees, *J. Algorithms* **3** (1982), 1–8.
- [Th65] R. Thom, Sur l’homologie des variétés algébriques réelles, in “Differential and Algebraic Topology” (S. S. Cairns, Ed.), Princeton Univ. Press, Princeton, 1965.
- [Y82] A. Yao, On parallel computation for the Knapsack problem, *J. Assoc. Comput. Mach.* **29** (1982), 898–903.
- [Y92] A. Yao, Algebraic decision trees and Euler characteristics, *Theoret. Comput. Sci.* **141** (1995), 133–150.